U.S. Department of Justice

United States Attorney
Eastern District of New York

271 Cadman Plaza East
Brooklyn, New York 11201

January 11, 2011

By Hand and ECF

The Honorable Nicholas G. Garaufis
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: In the Matter of an Application
Misc. Docket No. 10-0897

Dear Judge Garaufis:

On December 22, 2010, the government applied to United States Magistrate Judge James Orenstein, Eastern District of New York, for an order pursuant to 18 U.S.C. § 2703(d) authorizing the disclosure of recorded information identifying the base station towers and sectors that received transmissions from a specified telephone at the beginning and the end of calls or text message transmissions and the mobile switching center serving the telephone (the "historical cell-site location records") during any calls or text message transmissions for the period from September 1, 2010 until 11:00 a.m. on the date that the Court issued the requested order (the "Application"). On December 23, 2010, Judge Orenstein denied the Application. See In re Application, No. 10-MC-0897, Memorandum and Order, Dec. 23, 2010 (Orenstein II).

As recounted in his opinion, Judge Orenstein denied a similar application on August 27, 2010, relying principally on the reasoning of the D.C. Circuit in United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), a case concerning the prospective monitoring of a GPS tracking device on a vehicle and not historical cell-site location records. Judge Orenstein applied Maynard's reasoning to hold that the government must obtain a warrant to require a cellular telephone service provider to disclose historical cell-site location records. See In re Application, No. 10-MC-550, 2010 WL 3463132 (E.D.N.Y. Aug. 27, 2010) (Orenstein I) at *5.

On November 29, 2010, United States District Court Judge Roslynn R. Mauskopf entered an order reversing Judge Orenstein and granting the government's application in that case for an order under section 2703(d) compelling the production of the requested historical cell-site location records. Judge Mauskopf's order also indicated that a written memorandum would follow, but that opinion has not yet issued.

Notwithstanding Judge Mauskopf's reversal, and notwithstanding his acknowledgment that in the instant case the government has "proffered 'specific and articulable facts'" in conformity with the statute, Orenstein II at 1, Judge Orenstein's December 23 denial reasserts his earlier views, incorporating Orenstein I by reference. Judge Orenstein also advances new arguments in support of his renewed demand that the government seek a warrant in order to obtain historical cell-site location records.

As set forth below, Judge Orenstein's denial of the Application is, as before, unfounded and contrary to law. The government respectfully submits this letter requesting that the Court grant the government's Application.

A disclosure order under 18 U.S.C. § 2703(d) "may be issued by any court that is a court of competent jurisdiction." Therefore, the government may resubmit the Application to Your Honor as miscellaneous judge following its denial by Judge Orenstein. See, e.g., In re Application, 632 F. Supp. 2d 202, 203 (E.D.N.Y. 2008) ("Garaufis").

A. Background

The Application seeks an order authorizing the disclosure of recorded information identifying the base station towers and sectors that received transmissions from [redacted], a telephone issued by AT&T Wireless with IMSI Number [redacted] subscribed to by Kamal Abdallah at [redacted] (the "Subject Telephone"), at the beginning and the end of calls or text message transmissions, and the mobile switching center serving the Subject Telephone during any calls or text message transmissions. Accompanying the government's application were a proposed Order directed to the service provider and a proposed Order of Authorization.

In support of the Application, the government set forth specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and

material to an ongoing investigation, the standard set out for such applications in 18 U.S.C. § 2703(d). In particular, the government described its investigation into the possible violation of federal criminal laws, including bail jumping in violation of 18 U.S.C. § 3146(a)(1). Specifically, the Application alleged that the user of the Subject Telephone was an individual named Kamal Abdallah who was on pre-trial release from an indicted case in this District. After being charged and released on bail in this criminal case, Abdallah filed a voluntary petition for bankruptcy under Chapter 13 on November 2, 2010. As part of that petition, Abdallah filed a certification which stated, in substance, that he had not timely sought credit counseling, which was required under the bankruptcy laws, because he had recently been traveling abroad due to family and work obligations. Under his pre-trial release conditions, the defendant was required to surrender his passports and his travel was restricted to portions of Texas, Nevada and New York. Thus, the records sought in the Application were relevant to the government's investigation into whether Abdallah was planning to violate 18 U.S.C. § 3146(a)(1).[1]

B. Discussion

1. **Section 2703(d) is the proper statutory authority for applications and orders to compel the production of historical cell-site location records**

Pursuant to 18 U.S.C. § 2703(c)(1) and (d), a court may require a provider of electronic communication services to disclose records pertaining to customers to the government if the government offers "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an

---

[1] After submission of the Application to Judge Orenstein, Judge Bianco held a bail hearing in Abdallah's criminal case based on the statements made in Abdallah's certification. At the hearing, Abdallah stated that the certification was prepared by his bankruptcy lawyer and that its statements concerning his travel were not true. The government did not seek remand, and Abdallah's bail was continued. The government nevertheless is continuing its investigation into whether Abdallah has traveled out-of-the-country under an alias and still believes that the requested historical cell-site location records are relevant to that investigation. The government attaches its original application and proposed orders to this letter.

ongoing criminal investigation." As Judge Orenstein observes, courts have concluded widely that this statute applies to cell-site data. See Orenstein II at 1. Notably, this Court reached that same conclusion. See Garaufis, 632 F. Supp. at 206-07 (holding that prospective cell-site location information falls within the scope of the statute).

There is no dispute in this case that the government has met its statutory burden. As Judge Orenstein concedes, "[t]he government has proffered 'specific and articulable facts'" sufficient to satisfy section 2703(d). Orenstein II at 1.

2. Using a court order under section 2703(d) does not implicate the Fourth Amendment

The historical cell-site information the government seeks in this investigation is not in the possession of the suspect, but rather in the business records of a third party - the cell phone company. See In re Application, 509 F. Supp. 2d 76, 78 (D. Mass. 2007) (Stearns) (wireless carriers collect and retain cell-site location records "for among other business purposes, to assess roaming charges"). The Supreme Court has held that a customer has no privacy interest in business records of this kind.[2] Addressing a Fourth Amendment challenge to a third party subpoena for bank records, the Court held in United States v. Miller, 425 U.S. 435 (1976), that the bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession." Miller, 425 U.S. at 440; see also SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party . . . he cannot object if the third party conveys that information or records thereof to law enforcement authorities").

Thus, an individual has no Fourth Amendment-protected privacy interest in business records, such as cell-site usage information, that are kept, maintained and used by a cell phone company in the normal course of business. If anything, the privacy interest in cell-site information is even less than the privacy interest in a dialed phone number or bank records. The location and identity of the cell phone tower handling a customer's call is generated internally by the phone company. A customer's Fourth Amendment rights are not violated when the

---

[2] But for 18 U.S.C. § 2703(d), the records at issue in this case could be compelled via subpoena.

phone company reveals to the government its own records that were never in the possession of the customer.[3]

Further, even if it were the case that cell-site information is disclosed by the subscriber to the telephone company, the Supreme Court's reasoning in Smith v. Maryland leads to the same result. In that case, the Court held both that telephone users have no subjective expectation of privacy in dialed telephone numbers and also that any such expectation is not one that society is prepared to recognize as reasonable. See 442 U.S. at 742-44. The Court's reasoning applies equally to cell-site information. First, the Court stated: "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Id. at 742. Similarly, cell phone users understand that they must send a radio signal, which is received by a cell phone company's antenna in order to route their call to its intended recipient. (Indeed, cell phone users are intimately familiar with the relationship between call quality and radio signal strength, as typically indicated by a series of bars on their phones' displays.)

Second, under the reasoning of Smith v. Maryland, any subjective expectation of privacy in cell-site location records is unreasonable. The Supreme Court explicitly held that "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable." Id. at 743 (internal quotation omitted). It noted that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at 743-44. Thus, the user "voluntarily conveyed numerical information to the telephone company" and thereby "assumed the risk that the company would reveal to the police the numbers he dialed." Id. at 744. When a cell phone user transmits a signal to a cell tower for his call to be connected, he thereby assumes the risk that the cell phone provider will

---

[3] The same is true when a customer uses a bank ATM or a payphone on the street. By virtue of the transaction itself, which involves the company's own physical infrastructure, the company knows where the transaction takes place. Under Miller, records of such events do not implicate the Fourth Amendment, even though they disclose a customer's physical location to a far higher precision than cell-site records.

create its own internal record of which of its towers handles the call. Thus, it makes no difference if some users have never thought about how their cell phones work; a cell phone user can have no expectation of privacy in cell-site records.

Numerous courts have held these constitutional principles directly applicable to cell-site location records. See United States v. Velasquez, 2010 WL 4286276 at *5 (N.D. Cal. Oct. 22, 2010) (denying suppression); United States v. Benford, 2010 WL 1266507 at *3 (N.D. Ind. Mar. 26, 2010) (denying suppression); United States v. Jenious, No. 09-Cr-097 (E.D. Wis. Aug. 28, 2009) (unpublished); United States v. Suarez-Blanca, 2008 WL 4200156 at *23 (N.D. Ga. Mar. 26, 2008) (denying suppression); In re Application, 405 F. Supp. 2d 435, 449-50 (S.D.N.Y. 2005) (Gorenstein); State v. Marinello, 2010 WL 3893758 (La. App. Oct. 6, 2010) (denying suppression); Mitchell v. State, 25 So. 3d 632 (Fla. Dist. Ct. App. 2009) (denying suppression).

It is also well established that cell-site location records are not in any event so precise as to trigger potential Fourth Amendment concerns. As this Court held previously,

> The specter of . . . precise location tracking does not loom over this case, because the Government is seeking only information identifying the one antenna tower (and portion of such tower) receiving transmissions from the SUBJECT WIRELESS TELEPHONES at the beginning and end of calls made from those phones. . . . Such information, unlike the information revealed by triangulation or by more advanced communications devices like the iPhone, which contain Global Positioning System devices, is not precise enough to enable tracking of a telephone's movements within a home.

Garaufis, 632 F. Supp. 2d at 208.

3. Judge Orenstein's arguments in support of denial of the Application do not withstand scrutiny

In Orenstein II (and Orenstein I, incorporated by reference into the former), Judge Orenstein proffers various arguments in support of his conclusion that historical cell-site location records enjoy Fourth Amendment protection, and that the government therefore may not obtain them absent a warrant based on probable cause. As discussed below, these contentions lack merit, and this Court should - as Judge Mauskopf did in an identical challenge to Orenstein I - reverse Judge Orenstein and grant the requested section 2703(d) order.

a. United States v. Maynard does not apply to cell-site location records in any respect

Orenstein I relies almost entirely on the recent decision in United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010). In Maynard, the D.C. Circuit held that the use of a GPS tracking device to conduct "prolonged" monitoring (for 28 days) of the public movements of a suspect's vehicle violated the Fourth Amendment. Maynard, 615 F.3d at 556, 562. In doing so, the court of appeals attempted to distinguish United States v. Knotts, 460 U.S. 276 (1983), which holds squarely that monitoring the public movements of a vehicle by means of a tracking device is not a search under Fourth Amendment. The Maynard court distinguished Knotts as involving only the monitoring of a "discrete journey," Maynard, 615 F.3d at 556, and concluded that the month-long GPS surveillance of Jones's movements on public streets constituted a "dragnet-type law enforcement practice[,]" the legality of which the Supreme Court had reserved in Knotts. Id. at 556 (quoting Knotts, 460 U.S. at 283-284). The court also distinguished multiple federal appellate decisions that have held or suggested that GPS monitoring is not a search because those decisions did not specifically address the duration of the GPS surveillance. Id. at 557-58.

Maynard introduced a novel theory of what constitutes a "search" for purposes of the Fourth Amendment, which it derived from the "'mosaic theory' often invoked by the Government in cases involving national security information." Id. at 562. The court explained that, considered in the aggregate, Jones's movements were not "actually" exposed to public view because there was little "likelihood that a stranger would observe" all of the movements of Jones's Jeep during the month-long period. Id. at 560. The court also found that Jones had not "constructively" exposed to the public the aggregate of his Jeep's movements during the month-long period, reasoning that "[p]rolonged surveillance" is qualitatively different from a single instance of surveillance, because "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble." Id. at 562. Thus, the court concluded that, notwithstanding the fact that no particular instance of surveillance could be said to have violated the Fourth Amendment, Jones had a reasonable expectation of privacy in the public movements of his Jeep during the month-long period of the GPS surveillance in this case. Id. at 563. The court recognized that its ruling might call into question the use of prolonged visual surveillance, but expressly noted that the issue was not before it. Id. at 565.

None of these factors applies to historical cell-site information. The entire collection of data the government seeks has already been "actually exposed" to a third party: AT&T Wireless. The user of the Subject Telephone knows or should know that every time he places or receives a call, AT&T Wireless is advised of the cell tower being used, because the user knows that AT&T Wireless may later charge him for its services based in part on his location.

Furthermore, the entire collection of data does not reveal far more than the individual pieces of data it contains, nor does it reveal an intimate portrait of the user's life. The data reveals the general area where the user was when the user placed or received calls. It does not indicate where the user was within a particular building, and indeed likely would not even indicate what building the user was in or near. Moreover, the data does not include any information at all about where the user was during the vast majority of the day when he was not using the Subject Telephone. For all of these reasons, the user has no reasonable expectation of privacy in the historical cell-site records. The concerns that led the Maynard court to hold that the government must obtain a warrant before applying a GPS device to an individual's car do not apply to the government's application here.

Likewise, the reasoning of Maynard does not apply to historical cell-site records. There are at least four crucial differences between the data at issue in Maynard and that sought here.

First, in Maynard, law enforcement officers caused data to be created that would not otherwise have existed. By contrast, in this case the government seeks access to data that a third party already created, collected and maintained in the ordinary course of its business.

Second, the Maynard law enforcement officers covertly placed equipment upon the defendant's property to obtain location data. Here, the location data originated from equipment - a cell phone - that a person knowingly and voluntarily used and which equipment transmitted data as part of its normal operation. See United States v. Velasquez, 2010 WL 4286276 at *5 (N.D. Cal. Oct. 22, 2010) (denying motion to suppress historical cell-site records because "[t]he cell phone was not surreptitiously attached to an unwitting individual").

Third, in Maynard the GPS device provided data to the government 24 hours a day, allowing law enforcement officers to track the defendant in real time. Here, cell-site records exist only for the start and end times for periods in which the phone was engaged in a call or text message transmission, and are being sought only retrospectively.

Fourth, Maynard involved the most precise of all location information: GPS data. In this case, the government requests cell-site information, which is much less precise, as this court has held expressly. See Garaufis, 632 F. Supp. 2d at 208; Velasquez, 2010 WL at *5 ("[t]he privacy interests implicated [by historical cell-site records] pale in comparison to those implicated" by GPS tracking devices on vehicles).

Judge Orenstein rejected these arguments in Orenstein I. First, he reasoned that the fact that the government sought historical rather than prospective data did not affect whether the suspect had a reasonable expectation of privacy in the data. See 2010 WL 3463132 at *6. At the same time, however, Judge Orenstein conceded that prospective data can serve at least one important purpose for the government that historical data cannot: prospective data "may ease the task of commencing or continuing physical surveillance." Id. at *11 n.18. As a result, the government in Maynard could use the data it obtained to carry out additional investigation to create a far more "intimate picture of the subject's life," Maynard, 615 F.3d at 563, than would be available to the government here. The distinction between historical and prospective data thus directly impacts the Maynard court's rationale and weighs against applying that rationale to the current Application.

Judge Orenstein also dismisses the fact that Maynard addressed GPS information while the Application seeks less precise cell-site information. Judge Orenstein contends that, while cell-site records may not reveal a user's precise location, neither does GPS tracking: "GPS tracking by itself does not necessarily reveal a subject's '[r]epeated visits to church, a gym, a bar, or a bookie[.]'" Orenstein I, 2010 WL 3463132 at *10 (quoting Maynard, 615 F.3d at 562). Judge Orenstein notes that, if cell-site information does not reveal the user's location when he or she is not using the phone, neither did the GPS data in Maynard reveal where the defendant was when he was not driving. 2010 WL 3463132 at *13. The latter point ignores that the GPS device in Maynard transmitted data 24 hours a day, informing the government at least where the car was at all times; the historical cell-site records sought here would provide no information about the location of the user or the phone except

when calls are made or text messages are sent or received. In any event, both points demonstrate only that Maynard is not persuasive.[4] They do not suggest that this Court should extend Maynard's unpersuasive reasoning to the government's application for cell-site records.

Judge Orenstein further argues that 18 U.S.C. § 2703 does not distinguish among various forms of historical location data and reasoned that "any argument predicated on the relative precision of a given tracking method does nothing to validate the constitutionality of the [statute's] standard of 'specific and articulable facts' in the context of location tracking." 2010 WL 3463132 at *9 n.13. Similarly, Judge Orenstein declares that if the fact that a provider maintains cell-site records with respect to only one tower at each end of calls and text messages, and therefore that the Application seeks relatively imprecise data, is determinative, "then all future applications for [cell site data] must necessarily get bogged down in an inquiry into the precise record-keeping practices currently followed by the relevant service provider." Id.; see also id. at *10 n.16 (concluding government's argument concerning relative precision of cell-site records and GPS data "assures virtually instant obsolescence to a decision here in the government's favor" because cell-site records may be more precise in the future).

But this Court need not and should not evaluate the facial constitutionality of the statute in all of its hypothetical applications. See Sibron v. New York, 392 U.S. 40, 62 (1968) ("Our constitutional inquiry would not be furthered here by an attempt to pronounce judgment on the words of the statute [authorizing certain warrantless seizures]. We must confine our review instead to the reasonableness of the searches and seizures which underlie these two convictions."); see also

---

[4] Indeed, the latter point undermines the very premise of Maynard, that it was addressing the scenario upon which the Supreme Court reserved decision in Knotts. Maynard noted that Knotts rejected the defendant's argument that approving the GPS tracking used in that case would permit "'twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision,'" because if such law enforcement practices were eventually employed, "there will be time enough then to determine whether different constitutional principles may be applicable." Knotts, 460 U.S. at 283 (quoted in Maynard, 615 F.3d at 556). As Judge Orenstein noted, however, the GPS monitoring in Maynard did not constitute 24-hour surveillance of the defendant.

Sabri v. United States, 541 U.S. 600, 609 (2004) (noting disapprovingly that facial challenges "call for relaxing familiar requirements of standing, to allow a determination that the law would be unconstitutionally applied to different parties and different circumstances from those at hand."). In fact, this Court has rejected such efforts to litigate "hypothetical future case[s]" involving location records different from those requested in the instant Application. Garaufis, 632 F. Supp. 2d at 208.

Judge Orenstein asserts that, "in seeking to distinguish Maynard on the ground that [cell-site data] is not very precise, the government proves too much," because, after all, the government is seeking the data for a reason. Orenstein I, 2010 WL 3463132 at *11. It is true that the government believes the data is relevant to its investigation because it provides some information about the target's location. But maintaining that belief and observing that cell-site data is less precise than GPS data is not "hav[ing] it both ways," as Judge Orenstein proclaims. Id. It is simply recognizing historical cell-site data for whatever value it has, no more and no less - and as this Court has recognized, "[f]or obvious reasons, such [cell-site] information . . . is also useful to the Government as an investigatory tool" even though it is different from, and less precise than, GPS data. Garaufis, 632 F. Supp. 2d at 205 (citing In re Application, 460 F. Supp. 2d 448, 451-52 (S.D.N.Y. 2006) (Kaplan)).

Similarly, telephone toll records are less detailed than the content of telephone calls, but toll records nonetheless can further a government investigation and can be obtained without a search warrant. Judge Orenstein's rationale suggests that all useful evidence is protected by the Fourth Amendment, abandoning the well-established rule that the protection applies only when an individual has a reasonable expectation of privacy. See United States v. Hayes, 551 F.3d 138, 143 (2d Cir. 2008) ("A Fourth Amendment 'search,' however, does not occur unless the search invades an object or area where one has a subjective expectation of privacy that society is prepared to accept as objectively reasonable.") (citing Illinois v. Caballes, 543 U.S. 405, 408 (2005)).

Apart from the fact that Maynard has no bearing on the Application before this Court, it is in any event wrongly decided. Most obviously, "[a]lthough . . . continuous monitoring may capture quantitatively more information than brief stints of surveillance, the type of information collected is qualitatively the same." United States v. Sparks, 2010 WL 4595522 at *8 (D.

Mass. Nov. 10, 2010) (expressly rejecting the reasoning of Maynard); see also United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) ("The reasonable expectation of privacy as to a person's movements on the highway is, as concluded in Knotts, zero. The sum of an infinite number of zero-value parts is also zero.") (Sentelle, C.J., dissenting from denial of reh'g en banc in Maynard). Thus, as Maynard itself concedes, three other circuits have found that GPS monitoring of a vehicle's public movements do not violate the Fourth Amendment. See United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007), cert. denied, 128 S. Ct. 291 (2007).

In addition, the Maynard theory that otherwise permissible GPS monitoring can, when aggregated, violate the Fourth Amendment conflicts with the Supreme Court's analysis in United States v. Karo, 468 U.S. 705, 719-21 (1984) In Karo, the warrantless monitoring of a tracking device in a can of ether lasted for over four months. Id. at 709-10. The Supreme Court found that certain individual monitoring events during that period, i.e., those that revealed information about private spaces, were impermissible, but the Court's holding in no way depended upon the duration of the monitoring. Id. at 714-18. Indeed, the Court went on to analyze whether the warrant affidavit at issue, which was based in part upon the impermissible portions of the monitoring, nonetheless contained sufficient untainted evidence so as to establish probable cause under Franks v. Delaware, 438 U.S. 154 (1978). Id. at 719. The Court carved out the permissible portions of the monitoring (i.e., those that did not invade private space), and found that those portions, in combination with other evidence (e.g., visual surveillance), established probable cause for the warrant. In doing so, the Court expressed no concern about the four-month duration of the monitoring. Id. at 719-20. Thus, instead of suppressing the totality of the government's months-long monitoring, the Supreme Court explicitly rejected such an approach.

Maynard suffers from almost countless other practical and analytical defects. As catalogued by the court in Sparks,

> [t]he court in Maynard . . . leaves police officers with a rule that is vague and unworkable. It is unclear when surveillance becomes so prolonged as to have crossed the threshold and created this allegedly intrusive mosaic. What's more, conduct that is initially constitutionally sound could later be deemed

> impermissible if it becomes part of the aggregate. Finally . . . a rule prohibiting prolonged GPS surveillance due to the quantity or quality of information it accumulates would also incidentally outlaw visual surveillance and this Court is unwilling, and unable, to extend the reach of the Fourth Amendment that far.

2010 WL 4595522 at *8.

For all the reasons above, this Court should reverse Judge Orenstein and grant the Application.

b. The Wireless Communications and Public Safety Act of 1999

Orenstein I also relied upon the Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (Oct. 26, 1999) ("the WCPSA"), to conclude that cell phone users have a reasonable expectation of privacy in cell-site records. See Orenstein I, 2010 WL 3463132 at *8. This legislation, however, supports the opposite conclusion.

The WCPSA required that cell phone service providers adopt 911 as the number to be dialed to reach emergency services. See WCPSA § 3(a). It also permitted providers to disclose "call location information" to emergency services. WCPSA § 5(1); see also S. Rep. No. 106-138, at 7 (1999) ("This section requires the provision of call location information to emergency service personnel and data management services solely for the purpose of assisting in the delivery of emergency services."). It did so by amending 47 U.S.C. § 222, which requires telecommunications companies to "use, disclose, or permit access to" customer information only in their provision of the service from which the data was derived, "[e]xcept as required by law or with the approval of the customer" and for certain other purposes. 47 U.S.C. §§ 222(c)(1),(d). The WCPSA added the disclosure of "call location information" to emergency services to the list of other purposes for which telecommunications companies may disclose customer information. WCPSA § 5(1).

The WCPSA also added a new provision clarifying the pre-existing "approval of the customer" exception to the bar on use and disclosure of customer information. The new provision - cited by Judge Orenstein, Orenstein I, 2010 WL 3463132 at *8 - declares that, "without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to . . . call location

information." WCPSA § 5(2) (codified at 47 U.S.C. § 222(f)). Judge Orenstein views this new provision as demonstrating a congressional recognition and codification of a reasonable expectation of privacy in cell-site records.

He is mistaken. First, the phrase "except as required by law" of course includes an exception for criminal legal process, see Parastino v. Conestoga Tel. & Tel. Co., 1999 WL 636664, at *1-2 (E.D. Pa. Aug. 18, 1999) (dismissing lawsuit alleging violation of 47 U.S.C. § 222 because disclosure made pursuant to state court subpoena in criminal investigation), so the original language of the statute - left untouched by the amendment - contemplates disclosure to government investigators. Moreover, the amendment was enacted as part of a bill permitting the disclosure of call location information to government personnel. If anything, the WCPSA as a whole demonstrates that it is objectively unreasonable for anyone to maintain an expectation of privacy - at least vis-a-vis the government - in the data created by the use of a cell phone.

More importantly, statutory rights do not establish a Fourth Amendment expectation of privacy. On the contrary, the Supreme Court recently dismissed any such suggestion:

> Respondents point to no authority for the proposition that the existence of statutory protection renders a search per se unreasonable under the Fourth Amendment. And the precedents counsel otherwise. See Virginia v. Moore, 553 U.S. 164, 176 (2008) ("We conclude that warrantless arrests for crimes committed in the presence of an arresting officer are reasonable under the Constitution, and that while States are free to regulate such arrests however they desire, state restrictions do not alter the Fourth Amendment's protections."); California v. Greenwood, 486 U.S. 35, 43 (1988) ("We reject respondent Greenwood's alternative argument for affirmance: that his expectation of privacy in his garbage should be deemed reasonable as a matter of federal constitutional law because the warrantless search and seizure of his garbage was impermissible as a matter of California law.").

City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010). As the Fifth Circuit has observed in analyzing the Right to Financial Privacy Act,

> [w]hile it is evident that Congress has expanded individuals' right to privacy in bank records of their accounts, appellees are mistaken in their contention that the expansion is of constitutional dimensions. The rights created by Congress are statutory, not constitutional.

United States v. Kington, 801 F.2d 733, 737 (5th Cir. 1986) (emphasis added).

Thus, neither the WCPSA nor any other statute creates a reasonable expectation of privacy in historical cell-site records, and the Fourth Amendment does not therefore bar disclosure of such records pursuant to a 2703(d) order.

c. The Third Circuit's recent opinion does not support Judge Orenstein's claim that a warrant is required here

In addition to relying on Maynard, Judge Orenstein in Orenstein II bases his denial on additional precedent issued since Orenstein I. To begin with, he points to dicta in the Third Circuit's recent decision, In re Application, 620 F.3d 304 (3d Cir. 2010).[5] Without deciding the constitutional question, the Third Circuit remarked in passing that

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As [amicus] notes, it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information.

620 F.3d at 317 (emphasis in original).

---

[5] The main holding of the Third Circuit decision is that a magistrate judge has discretion - to be exercised "sparingly" - to require a probable cause showing when the government makes an application under section 2703(d). Id. at 319. Although we regard this result as incorrect, we do not address the question in this filing because Judge Orenstein appears to base his denial strictly on constitutional grounds. See Orenstein II at 1 ("granting the government's application would violate the Fourth Amendment"). The government stands ready to provide supplemental briefing on this issue if the Court desires it.

Aside from the fact that the Third Circuit's observation is dicta, it is also incorrect as a matter of constitutional law. In response to this very claim, the Supreme Court declared in Smith v. Maryland that

> [t]his argument does not withstand scrutiny. The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.

442 U.S. at 745.[6]

d. Smith II

Orenstein II also cites approvingly to a recent decision from a magistrate judge in another district holding that historical cell-site records are protected by the Fourth Amendment. See In re Application, 2010 WL 4286365 (S.D. Tex.

---

[6] Judge Orenstein asserts that - unlike placing a call or sending a text message - receiving a call or text message occurs "without any voluntary action" by the cell phone user. Orenstein I, 2010 WL 3463132 at *10 n.16. In fact, a cell phone user must voluntarily accept an incoming call, either by opening the phone or by pressing a button. Cell-site information is not recorded for calls that are answered by voicemail rather than by the cell phone user. Though it is true that a cell phone user takes no active step to receive a particular text message, he or she voluntarily signed up for text message service and would rarely if ever receive a text message without voluntarily making known to others that he or she used that form of communication, either by sending text messages or otherwise. And as several courts have observed, a user wishing to keep his location information private can stop disclosing it by simply turning off his phone. See United States v. Velasquez, 2010 WL 4286276 at *5 (N.D. Cal. Oct. 22, 2010) ("Cell phones are voluntarily carried by their users and may be turned on or off at will."); United States v. Navas, 2009 WL 1138020 at *5 (S.D.N.Y. Mar. 19, 2009); United States v. Skinner, 2007 WL 1556596 at *16 (E.D. Tenn. May 24, 2007); United States v. Amaral-Estrada, 2006 WL 3197181 at *13 (S.D. Ind. June 30, 2006).

Oct. 29, 2010) (Smith II).[7] Here, too, Judge Orenstein's reliance is misplaced.

Smith II relies heavily on Orenstein I. See, e.g., 2010 WL 4286365 at *8-10. As noted above, Orenstein I was reversed by Judge Mauskopf, and its reasoning is incompatible with this Court's prior decision in Garaufis, 632 F. Supp. 2d 202. Moreover, even assessed on its own merits the reasoning in Smith II is flawed and distinguishable from the present case for several reasons.

First, like Orenstein I, Smith II's conclusion that historical cell-site records are subject to Fourth Amendment protection is based primarily on the DC Circuit's decision in Maynard. Id. For the reasons set forth above, Maynard is inapplicable to an application for historical cell-site records.

Second, Smith II attempts to pin its Fourth Amendment conclusions on the Supreme Court's tracking device decision in United States v. Karo, 468 U.S. 705 (1984). See Smith II, 2010 WL 4286365 at *6-7. However, this Court has squarely rejected Judge Smith's claim that historical cell-site information implicates Karo. See Garaufis, 632 F. Supp. 2d at 208.

Third, the Court should reject the conclusion in Smith II that cell-site information is protected by the Fourth Amendment because it is not voluntarily conveyed by the user. As an initial matter, there is a significant factual distinction between the historical cell-site application at issue in Smith II and that at issue in the present case. Unlike the present Application, which only requests cell-site location at the beginning and end of calls and texts messages, the application at issue in Smith II sought cell-site information when the cellular telephone was in an "idle state." Smith II, 2010 WL 4286365 at *10. Thus, the government in the present case will only receive location information if the user of the Subject Telephone voluntarily placed or accepted a call or sent or received a text message during the relevant time period.

More broadly, the reasoning of Smith II simply proves too much. The court attempts to distinguish Miller by arguing that when a user "makes a call, she is not required to enter her own zip code, area code, or other location identifier." 2010 WL 4286365 at *12. But the same is true when a bank customer enters

---

[7] We note that Smith II is currently under review by a district court judge.

a bank vestibule and uses an ATM, or when a person uses a payphone on the street corner: in neither case does the customer affirmatively type in a location code. Rather, it is by virtue of the interaction itself - involving physical equipment, with a known location, owned by the bank or phone company - that the company knows (and makes a routine record of) where the transaction occurs. Such records fall squarely within the rule of Miller, and thus outside the protection of the Fourth Amendment. This same rule applies with equal force to a cell phone customer's use of a given cell tower. See e.g., United States v. Benford, 2010 WL 1266507 at *2 (N.D. Ind. Mar. 26, 2010) (holding Miller applicable to historical cell-site records and denying motion to suppress); Suarez-Blanca, 2008 WL 4200156 at *23 (same).

In addition, the three legal authorities that Smith II relies on in concluding that the Fourth Amendment protects cell-site data because it is not voluntarily conveyed either do not support that proposition or are inapplicable to the present case. Following Orenstein I, Smith II first relies on the WCPSA, which as demonstrated above does not, like any other statute, create a Fourth Amendment right where none otherwise exists.

Smith II next relies on the Sixth Circuit's decision in United States v. Forest, 355 F.3d 942 (6th Cir. 2004), vacated on other grounds sub nom. Garner v. United States, 543 U.S. 1100 (2005). In Forest, the defendant moved to suppress cell-site data obtained from the telephone provider based on several calls from a DEA agent to the defendant's cellular telephone on a particular day in order to reestablish visual contact with the defendant. Id. at 947. The court denied the motion to suppress, finding that there was no Fourth Amendment violation. Id. at 950-51. Smith II relies on the portion of Forest distinguishing that situation from that in Smith v. Maryland. The court stated "[u]nlike the defendant in Smith, [the defendant] points out that 'he did not voluntarily convey his cell-site data to anyone. In fact, he did not use his telephone. The agent dialed [the defendant's] phone number and the dialing caused [the defendant's] phone to send out signals." Id. at 951 (second emphasis in original). While Forest may have applied to the cell-site data sought in Smith II, it does not apply to the historical cell-site records sought in this case, which again only provide location information for past transactions when the user of the Subject Telephone either placed or received a telephone call or sent or received a text message.

The final legal authority relied on by Smith II is the Third Circuit's decision in In re Application, 620 F.3d 304 (3d

Cir. 2010). To be sure, the Third Circuit specifically rejected the premise of that portion of Smith II that the provision of cell-site data turns a cellular telephone into a tracking device. In re Application, 620 F.3d at 312-13 ("We therefore cannot accept the MJ's conclusion that [cell-site information] should be considered information from a tracking device that, for that reason, requires probable cause for its production."). In addition, as noted above, the Third Circuit expressly did not decide the constitutional question and its conclusion that cell-site information is not voluntarily provided is mere dicta. Accordingly, none of the authorities cited in Smith II support the conclusion in this case that the Fourth Amendment protects cell-site data because it is not voluntarily conveyed.

Finally, Smith II's factual analysis is flawed. Smith II begins with 50 paragraphs of "findings of fact" that address the structure of phone companies' cellular networks, the location information generated by the phone companies, the accuracy of the location information generated by the phone companies, and the kind of location information stored and retained by service providers. See 2010 WL 4286365 at *2-6. The court arrived at these "facts" by taking improper judicial notice of congressional testimony.

Under Rule 201 of the Federal Rules of Evidence, "[a] judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." As the Advisory Committee Notes to Rule 201 caution, "[a] high degree of indisputability is the essential prerequisite." Advisory Committee Note to Subdivision (a). Indeed, "the tradition has been one of caution in requiring that the matter be beyond reasonable controversy." Id. at Note to Subdivision (b). As the Fifth Circuit has repeatedly confirmed, "judicial notice applies to self-evident truths that no reasonable person could question, truisms that approach platitudes or banalities." Hardy v. Johns-Manville Sales Corp., 681 F.2d 334, 347 (5th Cir. 1982); id. at 348 ("The rule of judicial notice 'contemplates there is to be no evidence before the jury in disproof.' . . . Surely where there is evidence on both sides of an issue the matter is subject to reasonable dispute.")

Of the 50 paragraphs of the "findings of fact" in Smith II, only the first paragraph, which states that cellular phones use radio waves to communicate with the telephone network, is appropriate for judicial notice under Rule 201. The opinion

relies primarily on the congressional testimony of Matt Blaze, a computer science professor at the University of Pennsylvania. See Smith II, nn. 13-17, 19, 21-35, 37-40, 42-46, and 51-55. This testimony, which addresses both the structure of provider networks and their internal record keeping practices, addresses matters far from platitudes, banalities, or self-evident truths. The "findings of fact" are also inconsistent with other court decisions and findings of the FCC. See, e.g., In re Applications, 509 F. Supp. 2d 76, 78 n.3 (D. Mass. 2007) ("In urban areas, cell towers can be only hundreds of feet apart. In rural areas, towers are often ten miles or more apart."); In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, 15 FCC Rcd. 17442, 17462 (Sept. 8, 2000) (finding that a certain location-finding technique accurate to within 500-1000 meters "would be significantly more precise" than "the location of the cell site or sector receiving the call."). Given the differences between Professor Blaze's testimony, on one hand, and the findings of other courts and the FCC, the "findings of fact" are subject to reasonable dispute and therefore were not an appropriate subject for judicial notice. Adopting Professor Blaze's testimony as indisputable fact violates the principle that "[j]udicial notice is denied to disputable propositions found in testimony at government hearings." 1 Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence § 201.13[1][c] (McLaughlin ed., 2d ed. 2010).

Other "findings of fact" in Smith II, including paragraphs 41, 50, and portions of 42 and 49 are not even facts: they are opinions, hypothetical speculation, inferences, or predictions about the future. See 21B Wright and Graham, Federal Practice and Procedure § 5104 ("opinion-facts," including inferences and statements about the future, are not generally appropriate for judicial notice).

e. United States v. Warshak is equally irrelevant to the instant Application for historical cell-site location information

Orenstein II also invokes United States v. Warshak, 2010 WL 5071766 (6th Cir. Dec. 14, 2010), in support of his demand that the government seek a warrant. Like Maynard, the Warshak decision has no bearing on the issues presented by the Application.

In Warshak, the Sixth Circuit held that in general "the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment."

2010 WL 5071766 at *12 (emphasis added). The court reached this conclusion by analogizing an email message to the contents of a letter or phone conversation, each of which enjoys Fourth Amendment protection. Id. at *11.

In addition, the court distinguished United States v. Miller on two grounds:

> First, Miller involved simple business records, as opposed to the potentially unlimited variety of "confidential communications" at issue here. . . . Second, the bank depositor in Miller conveyed information to the bank so that the bank could put the information to use "in the ordinary course of business." By contrast, Warshak['s ISP] was an intermediary, not the intended recipient of the emails.

2010 WL 5071766 at *13 (emphasis in original).

This Court need not determine whether or not Warshak was correctly decided, for the simple reason that the court's bases for distinguishing Miller do not apply to historical cell-site location records. First and most obviously, cell-site records are "simple business records" kept in the ordinary course of a wireless provider's business activities.[8] See United States Telecomm. Ass'n v. FCC, 227 F.3d 450, 463 (D.C. Cir. 2000) (signals sent from cell phones to cell sites "are necessary to achieve communications between the caller and the party he or she is calling") (quoting brief of FCC); United States v. Suarez-Blanca, 2008 WL 4200156 at *8 (N.D. Ga. Apr. 21, 2008) (finding that "historical cell site information is akin to other business records maintained in the course of business" and denying motion to suppress on Fourth Amendment grounds).

More importantly, cell-site records do not constitute the contents of a communication. See In re Application, 620 F.3d 304, 306 (3d Cir. 2010) ("The Government does not here seek disclosure of the contents of wire or electronic communications. Instead, the Government seeks what is referred to in the statute as "a record or other information pertaining to a subscriber to or customer of such service" ....); accord Garaufis, 632 F. Supp. 2d at 206. Unlike the contents of an email message, historical cell-site records lack the capacity to embody a "potentially

---

[8] If these records were not kept in the ordinary course of business, there would no historical records for the government to obtain in the first place.

unlimited variety of 'confidential communications'," but instead invariably convey "only information identifying the one antenna tower (and portion of such tower) receiving transmissions" from a suspect's wireless phone. Garaufis, 632 F. Supp. 2d at 208.

Finally, the Warshak court makes much of the fact that an email customer's ISP is a mere intermediary, and not the intended recipient of the customer's email messages. Cell-site information, by contrast, is not intended for some other private communicant; rather, it exists solely to be used by the wireless carrier as an essential ingredient in providing service to the customer.

Conclusion

For these reasons, the government respectfully requests that its Application for historical cell-site location records be granted based on its offering of specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation.

Respectfully submitted,

LORETTA E. LYNCH
United States Attorney

By: /s/
Scott Klugman
Assistant U.S. Attorney
(718) 254-6461

Mark Eckenwiler
Associate Director, Office of
Enforcement Operations
Criminal Division

Encl.

cc: Clerk of Court (NGG) (w/o encl.)